SEALED

United States District Court

NORTHERN DISTRICT OF TEXAS

In the Matter of the Search of
(Name, address or Brief description of person, property or premises to be searched)

1730 BRENT COURT
GRAND PRAIRIE, TEXAS 75051

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 3:15-MJ- 195-BN

I Special Agent Marya Wilkerson being duly sworn depose and say:

I am a(n) Special Agent with Federal Bureau of Investigation (FBI) and have reason to believe that on the person of or XX on the property or premises known as (name, description and/or location)

(SEE ATTACHMENT A).

in the NORTHERN District of TEXAS there is now concealed a certain person or property, namely (describe the person or property to be seized)

(SEE ATTACHMENT B).

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)
property that constitutes evidence of the commission of a crime, contraband, the fruits of crime, and is, otherwise, criminally possessed, **concerning a violation of Title** 18 **United States code, Section(s)** 2252 and 2252A. **The facts to support a finding of Probable Cause are as follows:**

(SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT MARYA WILKERSON).

Continued on the attached sheet and made a part hereof. XX **Yes** _ **No**

Signature of Affiant
MARYA WILKERSON
Special Agent, FBI

Sworn to before me, and subscribed in my presence

March 26, 2015 **Date** at **Dallas, Texas** **City and State**

DAVID L. HORAN
United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT 1730 Brent Court Grand Prairie, TX 75051	)))))	**FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Marya Wilkerson, a Special Agent with the Federal Bureau of Investigation, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since April 2008. I am currently assigned to the Dallas, Texas, Division located at One Justice Way, Dallas, Texas, 75220. Prior to becoming a Special Agent, I was employed as an Assistant District Attorney for the Knox County District Attorney's Office for approximately four and a half years. Since joining the FBI, I have been involved in investigations of public corruption, white collar crimes, and crimes involving the exploitation of children through the Internet. I am currently assigned to investigate crimes involving the sexual exploitation of children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations, to include multiple search warrants and interviews with individuals participating in the trading of child pornography. I have also received training relating to the Innocent Images National Initiative (IINI), FBI

Cyber Crime Program, which includes training in the investigation and enforcement of federal child pornography laws in which computers are used as the means for receiving, transmitting, and storing child pornography. As a Special Agent, I am authorized to investigate violations of Federal law, including receipt, possession, and distribution of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A.

2. This affidavit is in support of an application for a search warrant for information associated with the Internet account registered to an individual with the initials "H.M.," (hereafter referred to as H.M.), located at 1730 Brent Court, Grand Prairie, Texas, 75051. As will be shown below, there is probable cause to believe that an individual using an internet account registered to H.M has possessed, transported, and/or distributed child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. I submit this application and affidavit in support of a search warrant authorizing a search of the residence located at 1730 Brent Court, Grand Prairie, Texas, 75051 (the "premises"), as further described in Attachment A incorporated herein by reference. Located within the premises to be searched, I seek to seize evidence and instrumentalities of criminal violations, which relate to the knowing possession, transportation and distribution of child pornography. I request authority to search the entire premises, including the residential dwelling and any computer and computer media located therein, for items specified in Attachment B (which is incorporated herein by reference) which may be found, and to seize all items listed in Attachment B as instrumentalities and evidence of a crime.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence and instrumentalities of the violation of 18 U.S.C. §§ 2252 and 2252A, are presently located at 1730 Brent Court, Grand Prairie, Texas, 75051.

STATUTORY AUTHORITY

4. This investigation concerns alleged violations of 18 U.S.C. §§ 2252 and 2252A, relating to material involving the sexual exploitation of minors.

a. 18 U.S.C. § 2252(a)(1) prohibits knowingly transporting or shipping, using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mails, any visual depiction of minors engaging in sexually explicit conduct.

b. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly

reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct.

c. 18 U.S.C. § 2252(a)(4) prohibits possessing or knowingly accessing with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means, including by computer, if the producing of such visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct.

d. 18 U.S.C. § 2252A(a)(1) prohibits knowingly mailing, transporting, or shipping any child pornography using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

e. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or

f. distributing any child pornography that has been mailed, or using any means or facility or interstate commerce, shipped or transported in or

affecting interstate or foreign commerce by any means, including by computer; or knowingly receiving or distributing any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

g. 18 U.S.C. § 2252A(a)(3)(A) prohibits a person from knowingly reproducing child pornography for distribution through the mails, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

h. 18 U.S.C. § 2252A(a)(3)(B) prohibits knowingly advertising, promoting, presenting, distributing, or soliciting through the mail, or using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer, any material or purported material, in a manner that reflects the belief or is intended to cause another to believe, that the material is or contains a visual depiction of an actual minor engaging in sexually explicit conduct, or an obscene visual depiction of a minor engaging in sexually explicit conduct.

i. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, any book, magazine, periodical, film, videotape, computer disk, or other

material that contains an image of child pornography that has been mailed, shipped, or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

   a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

   b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has

been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

c. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to,

physical keys and locks).

e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. "Computer software" is digital information that can be interpreted by a computer and any of its related components

to direct the way it works. It commonly includes programs to run operating systems, applications, and utilities.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

i. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

j. "Peer-to-peer file-sharing" (P2P) is a method of communication available to Internet users through the use of special software. Computers link together through the Internet using this software, which allows sharing of digital files between users on the same network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches

for files that are currently being shared on another user's computer.

k. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

l. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

m. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form

(including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

6. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

7. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage and social

networking.

8. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

10. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even

in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

12. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that date remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block

of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

PEER TO PEER FILE SHARING

13. A growing phenomenon on the Internet is peer-to-peer file-sharing (P2P).

14. P2P allows individuals to meet each other through the Internet, engage in social networking and trade files.

15. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time.

16. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred between computers.

17. Third-party software is available to identify the IP address of the P2P

computer sending the file. Such software monitors and logs Internet and local network traffic.

18. Millions of computer users throughout the world use Peer-To-Peer (P2P) file sharing networks to share files containing music, graphics, movies and text. These networks have also become a popular way to collect and distribute child pornography. Any computer user who can connect to the Internet can download P2P application software, which is typically free, and use this software to share files on a P2P network.

19. P2P software users can search the P2P network by entering search terms into their P2P software to generate a list of available files that contain the search terms. For example, a person interested in obtaining child pornographic images would open the P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results, the file(s) he/she wants to download. The files are downloaded directly from the computer sharing the file. The downloaded files are stored in the area or directory previously designated by the user and/or the software. The downloaded files will remain in that same location until moved or deleted.

20. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source

computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. However, a user downloading a file often receives the entire file from one computer.

21. When a user on the P2P network offers a file to trade, the Peer-To-Peer software used by law enforcement calculates a "hash value" of the file using a SHA-1 hash. A hash is a mathematical function that converts the data that comprises the contents of a file into an alphanumeric value. This value is unique to every file. A person may copy a file and rename it but if it is an exact copy, regardless of the name of the file, it will have the same hash value.

22. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology, along with the National Security Agency, as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States of America has adopted the SHA-1 hash algorithm described herein as a Federal Information Processing Standard.

23. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA-1 operation results in the creation of an associated hash value often referred to as a digital signature. By comparing these hash values, one can determine whether two files are identical with a precision that greatly exceeds 99.9999 percent certainty.

24. An investigator can examine the SHA-1 hash values of files being traded on the P2P network and determine if they are the same as the hash value of a file known

to be child pornography. The investigator is able to do this by comparing the hash value associated with a file offered on the P2P network with hash values of movies or images of child pornography identified from previous investigations. The use of SHA-1 hash values for the matching of movies and images has proven to be extremely reliable. The investigator can then verify the contents of the file by viewing a copy of the file that has the same hash value from a library of child pornography files kept by the investigator.

25. ARES is a popular P2P file sharing network. The strength of the ARES Network is that it bases all of its file shares on SHA-1. As with most, if not all P2P file transfers, a file transfer conducted on the ARES P2P network is assisted by a reference to an IP address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers.

26. The computer running the file sharing application, in this case ARES, has an IP address assigned to it while it is on the internet. Investigators are able to see the IP address of any computer system sharing files. Investigators can then search public records (ARIN.net) that are available on the Internet to determine the Internet service provider who assigned that IP address. Based upon the IP address assigned to the computer sharing files, subscriber information can be obtained from the ISP.

27. Based upon my training and experience, and conversations I've had with other law enforcement officers, the ARES network is being used to trade digital files,

including still images and movie files, of child pornography.

28. The ARES network is an open source public file-sharing network. Most computers that are part of this network are referred to as nodes. A node can simultaneously provide files to others on the same network while downloading files from other nodes. Nodes may be elevated to temporary indexing servers referred to as "supernodes." Supernodes increase the efficiency of the ARES network by maintaining an index of the contents of network users. ARES users query supernodes for files and are directed to one or more nodes sharing that file. There are many supernodes on the network, if one shuts down the network continues to operate.

29. The ARES network can be accessed by computers running many different programs, some of which include the original ARES Galaxy program, and derivatives compiled from the source code which is open source and freely available and are often referred to as client programs. These client programs share common protocols for network access and file sharing. However, the user interface, features, and configuration may vary between versions of the same software.

30. During the installation of an ARES client program, various settings are established which configure the host computer to share files. Depending upon the specific client program used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed. Typically, a setting establishes the location of one or more directories or folders whose contents (files) are made available to download by other ARES users. This location is commonly referred to as the "My Shared Folder" and in many versions is defaulted to

be on the computer's "Desktop."

31. The ARES client software processes files located in a user's shared directory before they are available to be shared. As part of this processing, a SHA-1 hash value is computed for each file in the user's shared directory.

32. The ARES network uses SHA-1 values to improve network efficiency. Users may receive a selected file from numerous sources by accepting segments of the file from multiple users and then reassembling the complete file on the local computer. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. The network uses SHA-1 values to ensure exact copies of the same file are used during this process.

33. Upon connecting to the ARES network, a list of shared files, descriptive information, and the files associated SHA-1 values are sent to supernodes. This allows other users to locate these files. The frequency of updating information is dependent upon the client software being used and the ARES networking protocols. This information sent to the super-node is data about the file and not the actual file. The file remains on the user's computer. In this capacity, the supernode acts as a pointer to the files located on a user's computer.

34. When a download of a file is initiated, the user is presented with a list of users (nodes) who told the ARES network that they have the requested file available for others to download. Typically, the supernodes and hosts computers on the network return this list containing node information and the IP addresses of computers which reported they have the same file (based on SHA-1 comparison) or in some

instances portions of the same file available to others to download. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known actual child pornography.

35. Obtaining files from the ARES network, as described herein, returns the candidate list, including IP addresses, which can be used to identify the location of computers. Although the IP address is not usually visible to the end user in the common ARES clients, it is returned and used by the software to initiate the download.

36. Law Enforcement has modified the ARES program to allow the downloading of a file from a single IP address as well as displaying the IP address, which is known to all ARES clients but not displayed.

37. When users on the ARES network conduct keyword searches, users sharing files matching the keyword, can be found. If the user sharing the file is not busy sharing with other ARES clients, the user could then download the shared files. When conducting investigations on the ARES network, law enforcement investigator can download files suspected of child pornography and then view the file(s) in order to describe it/them. If the sharing client is too busy to share files with an investigator, the investigator can use the SHA-1 hash of the file and compare the hash value to known child pornography images/videos. If the SHA-1 hash value matches, the investigator can rely on this hashing to identify the file being shared as child pornography, even without downloading the file.

BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE

38. On or about February 8, 2015, Task Force Officer (TFO) Jeffrey Rich conducted an investigation into the sharing of child pornography files on the ARES P2P file-sharing network. TFO Rich identified a computer with the IP address 108.234.18.116 as a potential candidate (source) for sharing multiple files of investigative interest on this date. TFO Rich directed his investigation to this computer at IP address 108.234.18.116 because it had been recently detected containing files of interest by investigators conducting keyword searches or hash value searches for files related to child abuse material, including child pornography, on the ARES network.

39. On February 8, 2015, TFO Rich downloaded a total of eleven completed files, of which nine video files were of child pornography. These downloaded files were from a sharing client using the IP address 108.234.18.116, which was recorded along with the date, time, and hash value of the file transfer.

40. These files were downloaded using a single-source program, meaning that the files were downloaded directly from IP address 108.234.18.116 on February 8, 2015. The downloaded files that depicted child pornography are described as follows:

File Name	File Description
(pthc) marissa aka feb3303 (new)(2).mpeg	This video file shows a prepubescent female child with brown hair, who is lying on a bed with a white cover. During the video, an adult male places his penis

	in the child's vagina.
!_new_!_(pthc)_veronika_05114_sam-ann.mpg	This video file shows a prepubescent female lying on a bed with her legs spread open to expose her genitals. A teenage male has his tongue placed on the female child's genitals.
KTGW50HNJZJRIYLBZLCDTY2FSTAB6ZWU.mpg	This video file shows a pubescent female child, with minimal breast development, wearing black socks and lying on a bed. The female child's mouth is on an adult male's penis.

41. Also, additional files were downloaded using a single-source program, meaning that the files were downloaded directly from IP address 108.234.18.116. These files were recognized as incomplete because the complete file was not downloaded, which is sometimes due to the transfer of a large video file; however, the files are files of investigative interest that were being made available by the suspect's computer utilizing the above IP address. In addition, this Affiant reviewed the contents of the incomplete files of investigative interest and the downloaded files are described as follows:

a. On or about February 8, 2015, the below file was downloaded partially from IP address 108.234.18.116. Of note, this file was incomplete because the system timed out during the download after receiving a partial download:

File Name	File Description
__ARESTRA__pthc 2012 amanda 8y nude show webcam (expuntitos).flv* *Of note, Ares will pre-pend the actual file name with "___ARESTRA___" (short for ARES Temporary Resource Allocation"). When the file is completed the pre-fix is simply removed.	This video file shows a prepubescent female child wearing a blue bathing suit bottom. The video file is focused on the child's genital area. The female child places her hand underneath her bathing suit and rubs her genital area.

42. A search of the American Registry for Internet Numbers (ARIN) online database indicated that IP address 108.234.18.116 is registered to the Internet Service Provider (ISP) of AT&T Internet Services. On February 9, 2015, a Collin County search warrant was served to AT&T to obtain electronic communications and subscriber records for the subscriber of IP address 108.234.18.116 between the time period of April 17, 2014, 7:47:16 PM CT and February 8, 2015 7:59:19 PM CT. Results from the search warrant sent to AT&T revealed that the IP address was assigned to an account registered to H.M, with the service address of 1730 Brent Court, Grand Prairie, Texas, 75051. AT&T also provided that this internet account with this specific I.P. address, 108.234.18.116, at 1730 Brent Court, Grand Prairie, Texas, 75051, had been activated on April 17, 2012.

43. Affiant has searched various records indices for information regarding H.M and 1730 Brent Court, Grand Prairie, Texas, 75051:

a. A Choicepoint Clear Report indicates that H.M. has an active address for

1730 Brent Court, Grand Prairie, Texas, 75051.

b. Dallas Central Appraisal District shows that H.M. is the owner for 1730 Brent Court, Grand Prairie, Texas, 75051.

44. On March 24, 2015, a physical surveillance of the premises was conducted. The premise at 1730 Brent Court, Grand Prairie, Texas, 75051, is a single family residence. The premise is described as a light colored brick residence with a cream colored garage. The numbers "1730" are on the residence above the garage. (See attached photographs and description in Attachment A, incorporated by reference).

45. In addition, during the physical surveillance on March 24, 2015, vehicles belonging to H.M. and a relative of H.M. were located in the driveway.

46. I am aware that many computers and electronic storage devices today, such as laptop computers, tablets, telephones, external drives and thumb drives, are portable. I also know from my training and experience that these devices are often stored in vehicles to prevent other users in the home from discovering the existence of the child pornography collection. Therefore, this application seeks permission to search vehicles located at or near the premises that fall under the dominion and control of the person or persons associated with said premises. The search of these vehicles is to include all internal and external compartments and all containers that may be associated with the storage of child pornographic materials or their instrumentalities contained within the aforementioned vehicles.

CHILD PORNOGRAPY COLLECTOR CHARACTERISTICS

47. Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing

lists, child erotica[1], and videotapes for many years.

d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

48. Based on this investigation, an individual utilizing the Internet at 1730 Brent Court, Grand Prairie, Texas, 75051, exhibits the common characteristics

[1] "Child erotica," as used in this affidavit, is defined as materials or items that are sexually arousing to certain individuals but which are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.

described above of someone involved in the distribution, transportation, receipt, possession and collection of child pornography, or the attempted distribution, transportation, receipt, or possession of child pornography. The user of IP address 108.234.18.116 has been known to law enforcement to have been utilizing the ARES P2P network to share child pornography with this IP address as early as April 6, 2014. Some of these files' hash values are known matches to identified child victims of sexual exploitation and the other files contain filenames indicative of child pornography or are files previously identified by law enforcement as meeting state or federal definitions of child pornography. Furthermore, these shared files mainly consist of videos or images of pubescent and prepubescent females and, therefore, show a specific predilection of this individual to be sexually interested in female children. In addition, law enforcement is aware that the user of IP address 108.234.18.116 has been actively sharing child pornography as of March 24, 2015.

49. Moreover, this shared collection has grown from 24 files of investigative interest on April 17, 2014, to as many as 424 files of investigative interest on March 24, 2015. In addition, multiple files of the investigative files of interest, contain "pthc" as part of the file name. This Affiant is aware that "pthc" is short for "pre teen hard core," and is a frequent search term utilized by collectors of child pornography to locate additional such files. This could indicate that the individual utilizing I.P. Address 108.234.18.116 is searching the ARES P2P program for files containing "pthc," and, thus, the individual is expressing an interest in child pornography for "pre teen hard core." Based on these facts and those set forth in the Background of the

Investigation it is believed that the individual utilizing IP address 108.234.18.116 demonstrates the characteristics of a collector of child pornography.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

50. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even

computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

51. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

52. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

CONCLUSION

53. Based on the forgoing, I respectfully submit that there is probable cause to believe that an individual who resides at the residence described above is involved in possession, transportation and distribution of child pornography. I respectfully submit that there is probable cause to believe that an individual residing in the residence described above has violated 18 U.S.C. §§ 2252 and 2252A. Additionally, there is probable cause to believe that evidence and instrumentalities of criminal offenses, namely, violations of 18 U.S.C. §§ 2252 and 2252A, are located in the residence at 1730 Brent Court, Grand Prairie, Texas, 75051, and this evidence, listed in Attachment B is instrumentalities and evidence which is or has been used as the means of committing the foregoing offenses.

54. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Respectfully submitted,

Marya Wilkerson
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on March 26, 2015.

JUDGE DAVID L. HORAN
UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF TEXAS

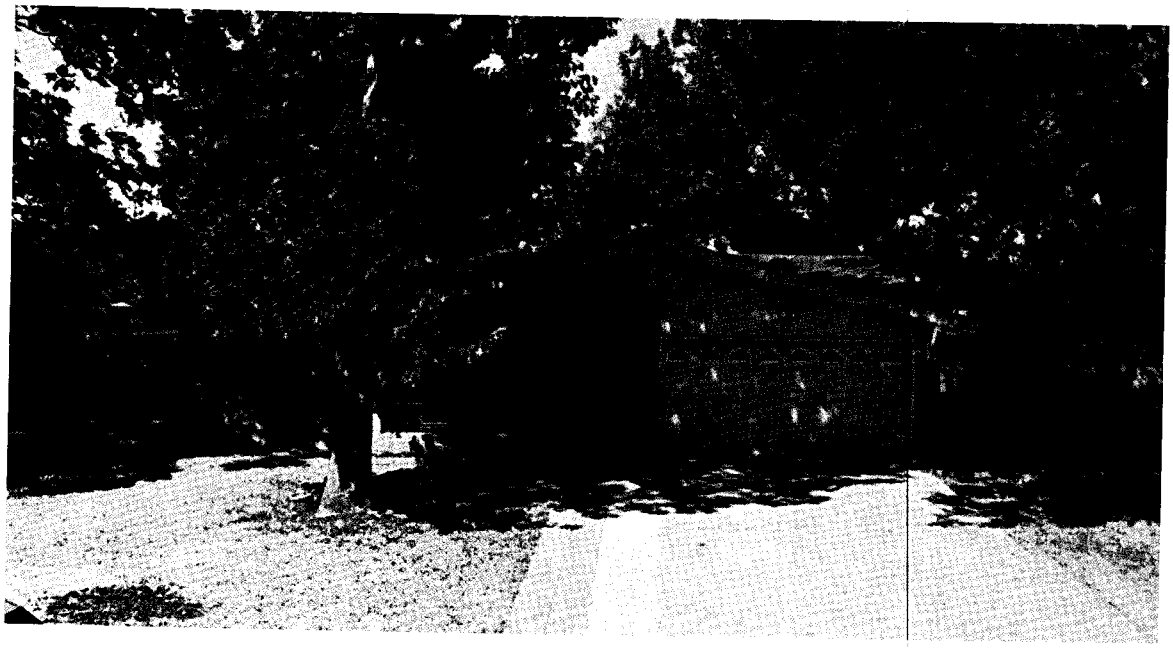
IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH OF)
THE PREMISES LOCATED AT)
)
1730 Brent Court) **FILED UNDER SEAL**
Grand Prairie, Texas 75051)
)

ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

On March 24, 2015, a physical surveillance of 1730 Brent Court, Grand Prairie, Texas, 75051, Dallas, Texas, 75287, was conducted. The premise at 1730 Brent Court, Grand Prairie, Texas, 75051, is a single family residence. The premise is described as a light colored brick residence with a cream colored garage. The numbers "1730" are on the residence above the garage. See below photo.



IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH OF)
THE PREMISES LOCATED AT)
)
1730 Brent Court)
Grand Prairie, Texas 75051)

FILED UNDER SEAL

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. Computer(s), computer system and related peripherals, computer hardware, computer software, computer related documentation, computer passwords and data security devices, cellular telephones, smartphones, tablet computers, e-readers, Apple Iphones, Apple Ipads, tapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Evidence of who used, owned, or controlled the computer(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, accounts of Internet Service Providers.

3. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or

addressed correspondence, rental or lease agreements, mortgage documents, rental or lease payments and credit card information, including, but not limited to, bills and payment records.

4. Any and all notes, documents, records, computer files or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), including communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography or membership in online groups, clubs, or services that provide or make accessible child pornography to members.

5. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

6. Any and all cameras, film, videotapes or other photographic equipment that may be used to commit or facilitate commission of violations of 18 U.S.C. §§ 2252 and 2252A.

7. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

8. Originals, copies and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

9. Motion picture films, videocassettes, and DVDs of visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

10. Registries regarding peer-to-peer file sharing software communications and participants in peer-to-peer file-sharing software networks.